العنوان:	دراسة تحليلية للمخترقين السعوديين : المخترقون، السعوديون، الاختراق، الحرب الرقمية، دراسة = Hacker, Saudi, Hacking, Cyberwar, Study
المصدر:	دراسات المعلومات
المؤلف الرئيسي:	الغثبر، خالد بن سليمان
مؤلفين آخرين:	الصبيح، أمل ناصر(مؤلف)
المجلد/العدد:	ع 10
محكمة:	نعم
التاريخ الميلادي:	2011
الشهر:	يناير
الصفحات:	243 - 270
رقم MD:	95019
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الهاكرز، السعودية، المخترقون السعوديون، الاختراق المعلوماتي، الحرب الرقمية، أمن المعلومات، الانترنت، الجرائم المعلوماتية، تكنولوجيا المعلومات ، السياسة المعلوماتية
رابط:	http://search.mandumah.com/Record/95019

دراسة تحليلية للمخترقين السعوديين

أ. خالد بن سليمان الغثبر
مركز التميز لأمن المعلومات
جامعة الملك سعود

أ. أمل ناصر الصبيح
مركز التميز لأمن المعلومات
جامعة الملك سعود

المخترقون، السعوديون، الاختراق، الحرب الرقمية، دراسة
Hacker, Saudi, Hacking, Cyberwar, Study

المستخلص:

يلج إلى شبكة الإنترنت يوماً بعد يوم كثير من المتصفحين؛ منهم الصغير والكير والمبتدئ والمتمرس؛ لشراء بضاعة أو الحصول على خدمة أو معلومة. وتتسابق الشركات والحكومات إلى تقديم خدماتها لمنسوبيها أو للزبائن من خلال هذه الشبكة المترابطة التي صار كثير من الناس يعتمدون عليها. وعلى الرغم من أهمية هذه الخدمة، إلا أن هناك كثيراً من المخاطر التي تحيط بها، وتكمن خطورتها في أنها تنفذ بحرفية ومارة. ومن تلك المخاطر المخترقون وما يقومون به من سرقة أو تعطيل خدمة أو تزوير أو ابتزاز أو غيرها من الجرائم المعلوماتية. ولكل دولة مخترقوها ولكن تتميز بعض الدول بوجود عدد أكبر وأكثر مهارة من المخترقين. وفي هذا البحث نحاول تسليط الضوء على المخترقين السعوديين والتعرف إلى ديموغرافيتهم ومهاراتهم وكذلك التعرف إلى تطلعاتهم المستقبلة، وذلك لفهم هذه الفئة والاستعداد للتعامل معها في الوقت الحالي وفي المستقبل.

١- المقدمة

لا يخفى على الجميع أهمية أمن المعلومات والحاجة الماسة إلى تطبيقه مع تزايد استخدام الأنظمة المعلوماتية في الجهات الحكومية وقطاع الأعمال وتبرز أهمية أمن المعلومات في مواجهة التحديات التي ينبغي أخذها في الاعتبار عند بناء أو تطوير أنظمة المعلومات والتي تنحصر في ثلاث محاور وهي:

أولاً: صحة المعلومات وسلامتها من التغيير.

ثانياً: سرية المعلومات، وأخيراً توافر المعلومة عند طلبها من الأشخاص المصرح لهم [٢].

وقد ساهم ظهور الإنترنت في تسهيل كثير من متطلبات الحياة وخاصة الأمور الإدارية والتنظيمية والمالية: ومع سرعة تطور الإنترنت وانتشاره ظهر كثير من الثغرات الأمنية التي تشكل تهديداً لا يقتصر على مستخدميها من الأفراد وإنما على اقتصاد وأمن الدول التي تعتمد عليه. ويعتبر الاختراق من أهم التحديات

التي تواجه أمن المعلومات في العصر الحالي والتي تتطلب تضافر الجهود من أجل مكافحة هذه الجريمة وتقليل خسائرها.

بحسب الإحصائية التي قدمتها شركة "كاسبرسكاي" لعمليات الهجمات الإلكترونية لعام ٢٠٠٨م في مختلف أنحاء العالم احتلت الصين المرتبة الأولى عالمياً في عدد عمليات الهجوم الإلكتروني وبنسبة ٥٣% من بين الدول، وجاءت مصر في المرتبة الثانية وبنسبة ١٥% من بين الدول وتلتها تركيا في المرتبة الثالثة وكانت السعودية في المرتبة التاسعة، وفي تقرير نفس الشركة لعام ٢٠٠٩م فقد ارتفعت مرتبة السعودية إلى المرتبة السابعة من بين الدول المعرضة للهجوم [١]. ووفقاً لدراسة أخرى أجريت مطلع عام ٢٠٠٩م لمعرفة مصادر الهجمات وجد أن الرياض تحتل المراكز الأولى في إطلاقها للهجمات بعد الولايات المتحدة الأمريكية [١٠].

ولدراسة الاختراق في المملكة العربية السعودية جاءت هذه الدراسة الاستطلاعية للتعرف إلى ديموغرافية المخترقين في المملكة العربية السعودية ومهاراتهم وكذلك التعرف إلى تطلعاتهم المستقبلية. وتبرز أهمية هذه الدراسة من خلال عدم وجود دراسات محلية مشابهة. كما تعتبر هذه الدراسة على حد علم الباحثين الدراسة الأولى التي تركز على المخترقين في السعودية. وستساعد هذه الدراسة على الخروج بحقائق وتوصيات عن المخترقين سوف تترجم إلى معلومات قيمة لمتخذي القرار.

وتتناول الورقة هذا البحث في خمسة أجزاء كما يلي: الجزء الأول سيتطرق لأنواع المخترقين والحرب الرقمية واستعراض لتجارب بعض الدول مع المخترقين. يليه الجزء الثاني الذي سيستعرض أهمية الدراسة وإجراءاتها، ثم الجزء الثالث سيحلل ويناقش نتائج الدراسة. أما الجزء الرابع فسيتناول المواقع الإلكترونية السعودية المؤرشفة في موقع زون اتش في الأعوام الفائتة. وفي الجزء الأخير سيختتم البحث بذكر بعضٍ من التوصيات.

٢- خلقية:

١/٢ أنواع المخترقين:

ينقسم الأشخاص الذين يهاجمون أنظمة الكمبيوتر والشبكات إلى عدة أقسام منها: المخترق، المخترق الخبيث، أطفال البريمجات، الجواسيس، الموظفون، إرهابيو الرقمية [٢]. ولكل قسم منهم توجهات ومهارات مختلفة سنأتي عليها بشيء من التفصيل.

المخترق:

تستخدم كلمة المخترق في معنيين: الأول هو معنى عام ويقصد به أي شخص يحاول الدخول إلى نظام الكمبيوتر أو إلى الشبكة بطريقة غير شرعية، وبهذا المفهوم تكون كلمة المخترق مرادفة لكلمة المهاجم. أما المعنى الآخر هو وصف للشخص الذي يمتلك مهارات حاسوبية عالية تمكنه من اختراق أنظمة الكمبيوتر، وهدفه هو اكتشاف ثغرات ومواطن ضعف النظام والبحث عن أي خلل قد يستخدمه المهاجمون في أغراض تخريبية، وتقديم تقارير وتوصيات؛ لتطوير الأمن في هذا النظام، فهدفه ليس هدفاً تخريبياً إنما هي مبادرة وإجراء وقائي لقياس مستوى أمن النظام ويسمى في هذه الحالة بالمخترق الأخلاقي.

المخترق الخبيث:

هو الشخص الذي لديه مهارات حاسوبية عالية ويخترق أنظمة الحواسيب والشبكات لأغراض تخريبية. بعكس المخترق الأخلاقي الذي يهدف إلى تطوير أمن النظام. يقوم المخترق الخبيث بإتلاف المعلومات وحرمان المستفيدين من الخدمات، وعمل أضرار خطيرة على أنظمة الحواسيب والشبكات. هذا الهجوم هو طلب للشهرة ومحاولة للتباهي بما يملكه المخترق من مهارات تمكنه من اختراق عدد كبير من الأجهزة أو المنافسة فيما بين المخترقين لكتابة برنامج خبيث يحدث ضرراً أكبر من غيره من البرامج.

أطفال البريمجات:

هم مستخدمو الحاسب من صغار السن أو المبتدئين الذين يحاولون فقط جذب الانتباه بعملهم التخريبي، يشبهون إلى حد كبير المخترقين الخبثاء الذين يحاولون الدخول إلى أنظمة الحواسيب؛ لإحداث أكبر ضرر ممكن، ولكن يختلفون عنهم بأنهم لا يملكون مهارات عالية لكتابة برنامج خبيث؛ إنما يقومون بتحميل برامج جاهزة للاختراق من الإنترنت.

الجواسيس:

هم أشخاص لديهم مهارات حاسوبية عالية وظفوها؛ لاختراق أجهزة الكمبيوتر وسرقة المعلومات. الجواسيس لا يقومون بالبحث العشوائي عن الأجهزة غير المؤمنة كما يفعل المخترقون والمخترقون الخبثاء وأطفال البريمجات، إنما يخترق جهازاً محدداً يحتوي على معلومات مهمة بدون إحداث أي ضرر أو لفت الانتباه.

الموظفون:

أكبر تهديد لأمن معلومات منظمة ما يأتي من مصدر غير متوقع ألا وهو من موظفي المنظمة نفسها. قد يخترق الموظفون أجهزة منظماتهم للأسباب التالية:

- لاكتشاف مواطن الضعف في أمن النظام كما يفعله المخترق الأخلاقي.

- قد يشعر الموظف أنه قد هضم حقه ومنع من الترقية فيود إرسال رسالة للفت الانتباه كما يفعله أطفال البريمجات، أو بقصد الثأر والانتقام.
- قد يغري منافسو المنظمة هذا الموظف بالمال لسرقة معلومات حساسة ويكون جاسوساً لهم.

إرهابيو الرقمية:

هم الذين يهاجمون البنية التحتية لأنظمة الحواسيب والشبكات ويلحقون أضراراً كبيرة بها؛ لأهداف سياسية أو دينية.

وهناك تقسيمات أخرى للمخترقين وهي: ذو القبعة البيضاء، ذو القبعة السوداء وذو القبعة الرمادية.

ذو القبعة البيضاء: هو شخص خبير في أمن المعلومات. يحاول الكشف عن مواطن ضعف النظام ويسعى لحمايته من أي تهديد خارجي. يستخدم صاحب القبعة البيضاء نفس الأدوات والطرق التي يستخدمها المخترق الخبيث، ولكنه يعمل في الحدود القانونية ويسمى بالمخترق الأخلاقي.

ذو القبعة السوداء: شخص ذو مهارات عالية في أنظمة الكمبيوتر. يقوم باختراق الأنظمة والشبكات بطرق غير قانونية لأغراض تخريبية مثل تغيير أو إتلاف المعلومات، نشير الفيروسات والديدان... الخ. وهدف صاحب القبعة السوداء من الاختراق إما مادي أو للتسلية أو لأغراض دينية وسياسية أو لأسباب اجتماعية.

ذو القبعة الرمادية: هو شخص يستخدم مهاراته في الاختراق القانوني وغير القانوني، أي أنه قد يكون ذا قبعة بيضاء في حالات وذا قبعة سوداء في حالات أخرى.

٢/٢ الحرب الرقمية:

أصبحت الهجمات الإلكترونية شكلاً من أشكال الحرب في القرن الحادي والعشرين وقد تشل دولاً بأكملها فقط بمهاجمة البنية التحتية لشبكة الإنترنت. ومن أشهر الأساليب المتبعة هو أسلوب حجم الخدمة عن المستفيدين، وذلك باستخدام كثير من الأجهزة المخترقة وإعطائها أوامر ببدء الهجوم في وقت محدد؛ فتغمر خوادم الشبكات المستهدفة بآلاف الرسائل والطلبات الوهمية وتحجب الخدمة عن المستفيدين.

الحرب على إستونيا:

في عام ٢٠٠٧م، تعرضت دولة إستونيا الواقعة بمنطقة البلطيق، والتي تعتبر من رواد "الحكومة الإلكترونية" في أوروبا، إلى وابل من الهجمات ضد مواقعها الإلكترونية وكانت الأهداف الرئيسية هي مواقع الرئاسة الإستونية وبرلمانها، الوزارات والمؤسسات الحكومية، الأحزاب السياسية، وكالات الأخبار، اثنين من أكبر البنوك، وشركات متخصصة في مجال الاتصالات [١١]. وقد اتهمت إستونيا روسيا التي لديها أعداد كبيرة من كتاب الفيروسيات المحترفين وقراصنة الكمبيوتر بشن تلك الهجمات.

وقد بدأت الهجمات الإلكترونية بالتزامن مع قرار لنقل النصب التذكاري السوفياتي للحرب العالمية الثانية – الجندي البرونزي – من موقع مركزي في عاصمة الدولة؛ لأن النصب تذكير بالقمع السوفيتي، وقد اعتبرت روسيا تحريكه إهانة؛ لأنها ذكرى للذين حاربوا النازية.

هذا الهجوم يسمى بحجب الخدمة الموزع، حيث تعرضت المواقع الإلكترونية فجأة إلى عشرات الآلاف من الزيارات مما أدى إلى تعطيل خوادم المواقع. وقد تدفقت الهجمات من كل أنحاء العالم لكن المسئولين الاستونيين وخبراء أمن المعلومات قالوا: إن عناوين الإنترنت للمهاجمين كان كثير منها مصدره روسياً لاسيما في مراحل الهجوم المبكرة وكان بعضها من مؤسسات الدولة الروسية. وقد أغلقت أستونيا الوصول الخارجي لمواقعها الإلكترونية لأجل وقف الاعتداءات.

أتهم رئيس الوزراء الإستوني مباشرة روسيا بالوقوف وراء ذلك الهجوم، لكن موسكو تنفي أي تورط لها في الهجمات [٥]. وقد قدم خبراء الإنترنت من حلف شمال الأطلسي والاتحاد الأوروبي المساعدة لتعقب الجناة. المسئول في حلف شمال الأطلسي لم يشر بأصابع الاتهام إلى أحد، ولكنه أكد أنه لا يمكن أن تكون هذه الأمور صادرة من عدد قليل من الأفراد [١١].

الحرب على جورجيا:

في عام ٢٠٠٨م، تعرضت جورجيا إلى هجوم رقمي على شبكة الإنترنت سبق الغزو الروسي لها. هذا الهجوم الذي يسمى بحجب الخدمة استهدف البنية التحتية للإنترنت وموقع الرئاسة في جورجيا ومواقع حكومية إلكترونية وشبكات عسكرية. يمثل هذا الهجوم مرحلة جديدة في تاريخ الحروب؛ لأنها المرة الأولى التي يشارك فيها الغزو البري هجوم رقمي. الهجوم كان منسقاً ومتطوراً جداً ولا يمكن أن يكون من عمل قراصنة مستقلين لأن حجمه يتطلب مشاركة عدد كبير من الموارد لا يمكن أن تقدمها إلا الدول.

من كان وراء الهجوم الرقمي غير معروف تماماً لكن الحكومة الجورجية اتهمت روسيا بالوقوف وراءه، وقد أنكرت الحكومة الروسية أي علاقة بالهجوم في النهاية جعل الهجوم الوصول إلى كثير من مواقع الحكومة على الإنترنت غير ممكن وحد من قدرة الحكومة على التواصل مع العالم خلال القتال مع روسيا [٢].

٣/٢ وضع المخترقين وموقف الحكومات:

١/٣/٢ الولايات المتحدة الأمريكية:

كجزء من أمن المعلومات الحكومية في الولايات المتحدة الأمريكية؛ صدر عام ٢٠٠٩م برنامج جديد أطلق عليه اسم "تحدي الولايات المتحدة الرقمي". للبحث عن ١٠٠٠٠ من المخترقين والمبدعين والمتميزين في التكنولوجيا من الشباب الأمريكي واستقطابهم لتجنيدهم في الجيش [٦]. هذا البرنامج هو نتيجة تضافر جهود مركز مكافحة الجريمة الرقمية في وزارة الدفاع الأمريكية، ومركز الدراسات الاستراتيجية والدولية، والقوات الجوي، ومعهد س. أ. ن. س.

يسعى هذا البرنامج إلى الاستفادة من المواهب والمهارات الوطنية غير المستغلة، عن طريق البحث عن المخترقين واكتشاف البارعين في التكنولوجيا من طلاب الثانوية والجامعة. ويهدف إلى حماية الولايات المتحدة الأمريكية من أي هجوم أو اختراق يهدد أمنها الرقمي عن طريق إنشاء جيل جديد من الخبراء والمتميزين في أمن المعلومات ووضعهم في المكان المناسب. هذا البرنامج يتألف من ثلاث منافسات وهي: تحدي التحقيق الرقمي، منافسة الهجوم على الشبكة والمنافسة الوطنية الرقمية [٣]. هذه المنافسات سوف تختبر مهارات المتسابقين في مهاجمة أهداف رقمية أو الدفاع عنها، سرقة المعلومات أو تتبع للكيفية التي تمت بها سرقة هذه المعلومات. وهذه المنافسات كالتالي:

- **تحدي التحقيق الرقمي**: هي منافسة أجراها معهد الجريمة الرقمية في وزارة الدفاع الأمريكية وتركز على الأدلة الجنائية الرقمية ومحاولة كشفها، وابتكار أدوات وتقنيات جديدة في التحقيق الرقمي، تعقب الاختراقات الرقمية، وإعادة بناء البيانات غير المكتملة.
- **منافسة الهجوم على الشبكة**: هي منافسة أجراها معهد س. ا. ن. س. صممت للتعرف إلى خبراء المستقبل في مجال أمن المعلومات واكتشاف مواطن ضعف شبكة افتراضية ومن ثم استغلالها وسرقة بياناتها [٨].

- **المنافسة الوطنية الرقمية**: هي منافسة أجرتها القوات الجوية الأمريكية؛ تركز على الدفاع عن أنظمة الحواسيب والشبكات وتحليل حالة الأمن فيها ومحاولة رد الهجمات أيضاً.

بالإضافة إلى ذلك، يعقد في أمريكا كل عام مؤتمر يعد الأكبر من نوعه، يطلق عليه القبعة السوداء، يجتمع فيه أكثر من ٤٠٠٠ شخص من مديري تقنية المعلومات، خبراء الصناعة، موظفي الحكومة، الأكاديميين، الباحثين والمخترقين. كان المؤتمر في بدايته تجمعاً للمخترقين فقط؛ لكنه تطور ليصبح مكاناً لمناقشة المعلومات التقنية في الأمن الرقمي وعرض أحدث البحوث الأمنية بالإضافة إلى إقامة كثير من الدوريات المختصة بالأمن الرقمي مثل: التشفير، تحليل البرامج الخبيثة، الهندسة العكسية والاختراق الأخلاقي [١٣].

٢/٣/٢ **تركيا**:

يعتبر المخترقون الأتراك من المتميزين في مجال الاختراق وكثير منهم يتعلم من المخترقين الروس مباشرة من خلال المنتديات الروسية؛ لأن لديهم معرفة باللغة الروسية هناك فئات متعددة من المخترقين الأتراك: منهم المخترقون المهتمون بالتكنولوجيا ومنهم المخترقون القوميون المتشددون ومنهم المخترقون أصحاب القبعة الخضراء أي ذوي الميول الإسلامي، وكذلك المخترقون المجرمون الذي همهم سرقة الأموال. غالباً تكون لدى الفرقة الأخيرة المذكورة مهارات تقنية دون المتوسط، مما يوقعهم في السجن بعد المتابعة من قبل الشرطة. بالنسبة للتجسس الصناعي والتجاري عن طريق الاختراق وسرقة البيانات الإلكترونية فإنه شائع في تركيا.

٣/٣/٢ **روسيا**:

وفقاً لما ذكره تقرير شركة أي ديفنس سوف تبقى روسيا الملاذ للمخترقين الأكثر تقدماً وخطورة في العالم، كما أن كثيراً من الأعمال التجارية الروسية وجدت هجمات حجب الخدمة واختراقات الشبكة تكتيكاً فعالاً ضد المنافسين. وقد نظر قادة في موسكو إلى المعلوماتية باعتبارها مصدر قوة سياسياً واستراتيجياً لابد من العناية به واستخدامه لتحقيق المصالح الوطنية[٧].

تصريحات المسئولين الروس تعطي دلالة واضحة على تبنيها فكرة الحرب الإلكترونية. منها ما أدلى به عضو اللجنة الأمنية للحكومة الروسية: "كثير من الصراعات في المستقبل القريب لن تحصل على أرض المعركة، وإنما على شبكة الإنترنت، وسنحارب بمساعدة جنود المعلومات، وهم المخترقون هذا يعني أن قوة صغيرة من المخترقين أقوى من عدة آلاف من القوات المسلحة الحالية" [٩].

٤/٣/٢ الصين:

تعد الصين من الدول المتقدمة في مجال التعليم والتوظيف الرقمي وتسعى لتحقيق "هيمنة إلكترونية" على كل خصومها بحلول عام ٢٠٥٠م لاسيما الولايات المتحدة وبريطانيا وروسيا وكوريا الجنوبية [٤]. و يجري جيش التحرير الشعبي الصيني المسابقات في الاختراق، لتحديد الموهوبين من المخترقين ومن ثم توظيفهم في جيشها الرقمي.

٣- الدراسة:

١/٣ أهداف الدراسة وأهميتها:

هذه الدراسة استطلاعية تهدف إلى التعرف إلى ديموغرافية المخترقين في المملكة العربية السعودية ومهاراتهم وكذلك التعرف إلى تطلعاتهم المستقبلة. أما أهمية هذه الدراسة فتبرز من خلال عدم وجود دراسات محلية مشابهة. كما تعتبر هذه الدراسة على حد علم الباحثين الدراسة الأولى التي تركز على المخترقين في السعودية. وستساعد هذه الدراسة على الخروج بحقائق وتوصيات عن المخترقين سوف تترجم إلى معلومات قيمة لمتخذي القرار.

٢/٣ أسئلة الدراسة:

تركز الدراسة على معرفة التالي:

- أعمار المخترقين ومستواهم التعليمي.
- مهارات المخترقين.
- أهداف المخترقين.
- طموح المخترقين.

٣/٣ أدوات الدراسة:

استخدم الباحثان أسلوب الاستبيان لجمع المعلومات من المخترقين، ويحتوي هذا الاستبيان على ٣٢ سؤالاً أتبع الباحثان نمط الأسئلة الاختيارية إما اختيار جواب واحد أو عدة أجوبة ممكنة، وأيضاً نمط الأسئلة المفتوحة التي تشجع المخترقين على إضافة آرائهم الخاصة. الأسئلة الأولى من الاستبيان كان الهدف منها جمع بعض المعلومات الديموغرافية عن المخترقين مثل: العمر، الجنس، المؤهل العلمي، الوظيفة والدخل. تلتها أسئلة ركزت على الهدف من الاختراق وأهم المواقع المستهدفة، كما طرحت أسئلة أخرى للتعرف إلى مهارات المخترقين وعلاقتهم ببعض، والجزء الأخير منها تناول تطلعات المخترقين المستقبلة.

وقد عرض الاستبيان على ذوي الخبرة من أجل التحكيم قبل نشره وتم إجراء اختبار أولي للاستبيان على مجموعة من المخترقين لأخذ آرائهم.

٤/٣ حدود وعينة الدراسة:

وجد الباحثان صعوبات في الوصول إلى المخترقين منها: صعوبة إقناع المشرفين على المنتديات على شبكة الإنترنت بالإعلان عن الاستبيان وأيضاً إقناع المخترق بالمشاركة؛ لخوفهم من التتبع ومن ثم المساءلة القانونية وأيضاً لعدم اهتمامهم بالدراسات والأبحاث. بالإضافة إلى أن بعض المنتديات الخاصة بالاختراق موقفة أو لا يرتادها السعوديون بكثرة. وقد تم الإعلان عن الاستبيان في منتديات كثيرة يرتادها المخترقون منها: منتدى قراصنة السعودية، منتدى خدمات العرب، منتدى أمان العرب، منتدى ترياق وكان عدد أعضائها على التوالي ١٩.١٤. عضو، ٢١٤.٣ عضو، ٥٦.٥٢. عضو. وأيضاً تعاون بعض المخترقين بنشر الاستبيان في شبكاتهم الخاصة وقد أرسلت الدعوة بالمشاركة لأكثر من ٦٧ شخصاً. وتم تعبئة الاستبيان إلكترونياً في الموقع الرسمي لمركز التميز لأمن المعلومات باستخدام كلمة المرور نشرت في المنتديات المذكورة سابقاً؛ لاستهداف المخترقين فقط ولمنع غيرهم من متصفحي الموقع. وقد بلغ عدد العينة ٨٣ مخترقاً من أصل ١٠٤ بعد إزالة التكرار والاقتصار على السعوديين الذين هم مجال البحث.

٥/٣ النتائج:

في هذا الجزء عرض لنتائج الاستبيان موزعاً على أربعة أقسام.

المعلومات الديموغرافية:

١- العمر:

العمر	العدد	النسبة
أقل من ١٨ سنة	٢٦	%٣١
من ١٩ إلى أقل من ٢٥ سنة	٤٦	%٥٦
٢٥ سنة فأكثر	١١	%١٣
المجموع	٨٣	%١٠٠

الجنس:

الجنس	العدد	النسبة
ذكر	٨٣	%١٠٠
أنثى	٠	%٠
المجموع	٨٣	%١٠٠

٣- المؤهل العلمي:

المؤهل العلمي	العدد	النسبة
ابتدائي	٢	%٢
متوسط	١٠	%١٢
ثانوي	٣٨	%٤٦
دبلوم	٨	%١٠
بكالوريوس	٢٠	%٢٤
دراسات عليا	٤	%٥
لم يحدد	١	%١
المجموع	٨٣	%١٠٠

٤- معرفة قراءة النصوص الإنجليزية:

معرفة قراءة النصوص الإنجليزية	العدد	النسبة
لا أجيد	٣	%٤
لابد من الترجمة	١٧	%٢٠
أجيد	٦٣	%٧٦
المجموع	٨٣	%١٠٠

٥- معرفة اللغات الأخرى:

معرفة اللغات الأخرى	العدد	النسبة
لا أجيد	٦٤	٧٧٪
أجيد	١٩	٢٣٪
المجموع	٨٣	١٠٠٪

٦- هل أنت موظف؟

هل أنت موظف	العدد	النسبة
نعم	٢٦	٣١٪
لا	٥٧	٦٩٪
المجموع	٨٣	١٠٠٪

٧- هل أنت مرتاح في وظيفتك؟

هل أنت مرتاح في وظيفتك	العدد	النسبة
نعم	١٨	٦٩٪
لا	٨	٣١٪
المجموع	٢٦	١٠٠٪

٨- الوظيفة في مجال تقنية المعلومات:

الوظيفة في مجال تقنية المعلومات	العدد	النسبة
نعم	١٧	٦٥٪
لا	٩	٣٥٪
المجموع	٢٦	١٠٠٪

٩- الدخل:

الدخل	العدد	النسبة
ليس لهم دخل	٤٣	٥٢%
أقل من ٤٠٠٠	١٨	٢٢%
بين ٤٠٠٠ و ٧٠٠٠	٨	٩%
أكثر من ٧٠٠٠	٨	٩%
المجموع	٨٣	١٠٠%

الاختراق وأهم المواقع المستهدفة:

١- هدف الاختراق:

الهدف	العدد	النسبة
الشهرة	٨	٨%
المال	٣	٣%
الانتقام	٨	٨%
التسلية	١٩	١٨%
الدفاع عن الدين – الوطن – فكر – عقيدة	٤٦	٤٥%
غير ذلك	١٨	١٨%

٢- هل تهاجم جميع المواقع بدون تحفظ؟

تهاجم بدون تحفظ	العدد	النسبة
نعم	١٠	١٢%
لا	٧٣	٨٨%
المجموع	٨٣	١٠٠%

٣- المواقع المستهدفة:

المواقع المستهدفة	العدد	النسبة
مواقع حكومية	١٠	%٥
بنوك ومتاجر	٦	%٣
منتديات	١٨	%١٠
مواقع بلدك	٥	%٣
مواقع أجنبية	٢٦	%١٤
مواقع إسرائيلية	٣٣	%١٤
مواقع إباحية	٣٢	%١٨
مواقع تهاجم الإسلام	٢٥	%١٨
تشارك بالرد على هجوم ضد الإسلام أو بلدك	٢٧	%١٥

٤- هل تتقاضى مقابل الاختراق؟

المال مقابل الاختراق	العدد	النسبة
نعم دائماً	٣	%٤
نعم أحياناً	١٢	%١٤
لا	٦٨	%٨٢
المجموع	٨٣	%١٠٠

مهارات المخترقين:

١- هل تجيد لغات البرمجة؟

إجادة لغات البرمجة	العدد	النسبة
نعم	٥٤	%٦٥
لا	٢٩	%٣٥
المجموع	٨٣	%١٠٠

٢- هل لديك مهارة البرمجة المرتجعة (Reengineering)؟

إجادة لغات البرمجة المرتجعة	العدد	النسبة
نعم	٢٨	٣٤٪
لا	٥٥	٦٦٪
المجموع	٨٣	١٠٠٪

٣- نظام التشغيل الذي تستخدمه وتفضله في أثناء الاختراق:

نظام التشغيل	العدد	النسبة
ويندوز	٤٧	٥٢٪
لينكس	٣٥	٣٩٪
ماك	٢	٢٪
بدون	٦	٧٪

٤- الأدوات التي تستخدمها للاختراق؟

الأداة	العدد	النسبة
الأحصنة الطروادة	٣٢	١٩٪
الهندسة الاجتماعية	٢١	١٢٪
معرفة مواطن الضعف	٣٢	١٨٪
استغلال اليوم الصفر	٣٣	١٩٪
حافظ نقرات لوحة المفاتيح	١٩	١١٪
طريقة الاستقصاء	٢١	١٢٪
الحواسيب المستغلة	١٥	٩٪

٥- ما المدة التي أمضيتها في الاختراقات؟

المدة	العدد	النسبة
أقل من سنة	٢٣	%٢٨
من سنة إلى أقل من ٣ سنوات	٢٤	%٢٩
٣ سنوات فأكثر	٣٦	%٤٣
المجموع	٨٣	%١٠٠

٦- ما عدد الساعات اليومية التي تقضيها في الاختراق أو محاولة الاختراق

عدد الساعات	العدد	النسبة
٨ ساعات في الأسبوع	٧	%٨
يومان في الأسبوع	٤	%٥
ثلاثة أيام في الأسبوع	٢	%٢
أربعة أيام في الأسبوع	٥	%٦
خمسة أيام في الأسبوع	٥	%٦
ستة أيام في الأسبوع	٤	%٥
١ – ٣ ساعات يومياً	٦	%٧
٤ – ٧ ساعات يومياً	١٤	%١٧
٨ – ١٢ ساعة يومياً	١٢	%١٥
١٣ ساعة أو أكثر يومياً	١٨	%١٨
بدون إجابة	٦	%٧
المجموع	٧٢	%١٠٠

٧- هل خبرتك في الاختراقات مبنية على:

الخبرة	العدد	النسبة
التعليم الذاتي	٦٨	٨٢٪
التعليم المنظم	١٥	١٨٪
المجموع	٨٣	١٠٠٪

٨- إذا كانت خبرتك في الاختراق مبنية على التعلم الذاتي فهل كانت:

الخبرة مبنية على	العدد	النسبة
اكتساب الخبرة عن طريق أحد المخترقين الذين سبقوك فيه.	٢٥	٢٣٪
الاستعانة بالمواقع والمنتديات التي تهتم بأمور الاختراق.	٦٣	٥٩٪
شراء الكتب المختصة في الأمن ومجال الاختراقات	١٩	١٨٪

٩- قيم مستواك في الاختراق:

المستوى	العدد	النسبة
مخترق ضعيف	٢٩	٧٪
مخترق صاحب أماني	٧	٩٪
مخترق مستجد	٦	٣٥٪
مخترق حقيقي	٢٥	٣٠٪
مخترق في القمة	١١	١٣٪
مخترق أخلاقي	١	١٪
بدون إجابة	٤	٥٪

١٠- كم مخترقاً سعودياً تعرفهم شخصياً؟

الفئة	العدد	النسبة
لا أعرف أحداً	١٨	٢٢٪
أقل من ١٠	٣٠	٣٦٪
بين ١٠ و٢٥	١٦	١٩٪
بين ٢٦ و٥٠	١١	١٣٪
أكثر من ٥٠	٨	١٠٪

١١- كم مخترقاً عربياً تعرفهم؟

الفئة	العدد	النسبة
لا أعرف أحد	١٩	٢٤٪
أقل من ١٠	٢٥	٣٠٪
بين ١٠ و٢٥	١٢	١٤٪
بين ٢٦ و٥٠	١٣	١٥٪
أكثر من ٥٠	١٤	١٧٪
المجموع	٨٣	١٠٠٪

١٢- كم مخترقاً أجنبياً تعرفهم؟

الفئة	العدد	النسبة
لا أعرف أحداً	٢٦	٣١٪
أقل من ١٠	٣٠	٣٦٪
بين ١٠ و٢٥	١٣	١٦٪
بين ٢٦ و٥٠	٢	٣٥٪
أكثر من ٥٠	٢	٢٪
المجموع	٨٣	١٠٠٪

١٣- هل تشارك بالمنتديات الحوارية؟

تشارك بالمنتديات الحوارية	العدد	النسبة
نعم	٣٤	%٤١
لا	٤٧	%٥٧
بدون إجابة	٢	%٢
المجموع	٨٣	%١٠٠

١٤- هل أنت تعمل ضمن مجموعة أم تعمل بشكل فردي؟

نوع العمل	العدد	النسبة
جماعي	٢٨	%٣٤
فردي	٥٥	%٦٦
المجموع	٨٣	%١٠٠

تطلعات المخترقين المستقبلة:

١- هل تود الاستمرار في الاختراقات أم تود استغلال هذه الموهبة في وظيفة في مجال أمن المعلومات؟

الاختيار	العدد	النسبة
الاستمرار في الاختراقات	٣٧	%٤٥
الوظيفة	٤٠	%٤٨
بدون إجابة	٦	%٧
المجموع	٨٣	%١٠٠

٢- هل تود أن نعقد معك مقابلة خاصة؟

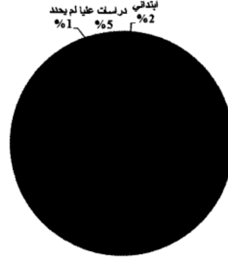
عقد مقابلة خاصة	العدد	النسبة
نعم	٣٦	٤٣%
لا	٤٠	٤٨%
بدون إجابة	٧	٩%
المجموع	٨٣	١٠٠%

٤. التحليل:

تبين من الدراسة أن المخترقين هم من الذكور بنسبة بلغت ١٠٠%. وقد احتللت الفئة العمرية بين ١٩ و٢٥ النسبة الأعلى حيث بلغت ٥٦% وبلغت نسبة المخترقين من الفئة العمرية ١٨ فأقل ٣١% ويعني ذلك أن الغالبية هم من الشباب أقل من ٢٥ سنة الشكل رقم (١). يأتي بعد ذلك مؤهلهم العلمي فنجد أن ٤٦% في مرحلة الثانوية تليها مرحلة البكالوريوس بنسبة ٢٤% الشكل رقم (٢). كما أوضح ٧٦% من عينة الدراسة معرفتهم قراءة النصوص الإنجليزية في حين أوضح ٢٣% من المشاركين في الدراسة معرفتهم بلغات أخرى كالفارسية والروسية والعبرية والألمانية وتعتبر هذه النسب جيدة في توضيح إمكانات المخترقين على التطور في التعليم والتواصل ورفع مهاراتهم مما قد يشكل تهديداً مستقبلياً.



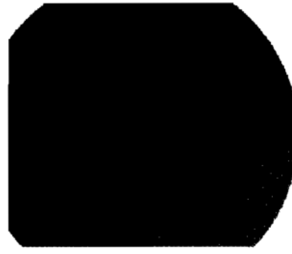
الشكل رقم (١): العمر



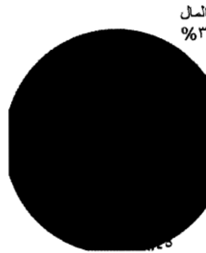
الشكل رقم (٢): المؤهل التعليمي لعينة الدراسة

بالنسبة للمجال الوظيفي فقد ذكر ٣١% من عينة الدراسة أنهم موظفون و٦٩% من الموظفين مرتاحون في وظائفهم كما بلغت نسبة الذين يعملون في تخصص تقنية المعلومات ٦٥%. وأتضح أيضاً أن النسبة الأعلى من عينة الدراسة ليس لها دخل مادي وتعادل ٥٢% تليها ٢٢% لديهم دخل أقل من ٤٠٠٠ الشكل رقم (٣). وهذا يدل على استنتاجين أحدهما أن أغلب المخترقين محل الدراسة ما زالوا طلاباً والاستنتاج الثاني هو أن العاطلين عن العمل من المخترقين أو الذين دخلهم قليل هم الفئة الأكثر وقد يشكلون تهديداً مستقبلياً إذا لم يكن لديهم اكتفاء مادي مناسب.

بينت نتائج الاستبيان أن هدف الاختراق لـ٤٥% من عينة الدراسة كان الدفاع عن الدين أو الوطن أو الفكر، تليها التسلية بنسبة ١٨% وتساوت الشهرة مع الانتقام بنسبة ٨%، وأخيراً كان الهدف المادي بنسبة قليلة تعادل ٣% الشكل رقم (٤). أما بالنسبة لأهم المواقع المستهدفة بالاختراق فنجد أن النسبة الكبرى منها (١٨%) تستهدف المواقع التي تهاجم الإسلام والنسبة الأقل (٢%) تستهدف البنوك والمتاجر الشكل رقم (٥). وتشير أيضاً النسبة المئوية المرتفعة، التي بلغت ٨٢%، بعدم تقاضي المال مقابل الاختراق إلى أن هدف أفراد عينة الدراسة من الاختراق ليس مادياً. كما أوضح ٨٨% من عينة الدراسة أنهم لا يهاجمون جميع المواقع بدون تحفظ. وكل هذه النتائج تشير إلى أن المخترقين السعوديين ليسوا كمثل المخترقين في دول أخرى في استهدافهم الجوانب المالية من سرقة بيانات أو أموال أو حتى امتهان الاختراق كمصدر رزق. وعليه فإن الخطر من المخترقين الحاليين ليس عالياً ولكن متى ما تغيرت أهداف المخترقين في المستقبل فإن ذلك قد يشكل تهديداً على المؤسسات المالية وقطاع الأعمال في السعودية.



الشكل رقم (٣): الدخل



الشكل رقم (٤): أهداف الاختراق

بالنسبة لمهارات المخترقين، فقد طرح سؤال يتضمن مستويات كثيرة من الاختراق وطلب من أفراد العينة تقييم مستوياتهم وهي كالتالي:

مخترق ضعيف: يخلط مشاهدة الاختراق بالحقائق المختلفة، معلوماته مبعثرة جداً، يحاول إبهار الناس العاديين بالكلمات الكبيرة. أعظم إنجازاته تشغيل برنامج تجسس في كمبيوتر شخص آخر عن طريق برامج محادثة ويقوم بحذف ملفاتهم.

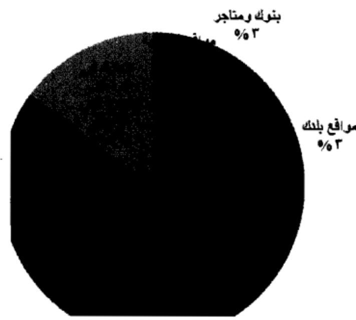
مخترق صاحب أماني: يتمنى أن يكون مخترقاً، ويريد المعرفة أكثر فيبدأ في قراءة دروس الاختراق ويبحث عن الأشياء المتعلقة بالمخترقين.

مخترق مستجد: الذي بدأ في تحقيق أمنيته، ووجد أن الاختراق أكثر من التسلل لأجهزة الكمبيوتر الشخصية، وأن الأمور أصبحت إلى حد ما فلسفة، أو أسلوب حياة ويحاول أن يفهم التكتيك الأساس للاختراق ويكتشف أن هناك برامج مساعدة يستطيع أن يستغلها ويحاول بواسطتها اقتحام أي نظام.

مخترق حقيقي: من الصعب أن تقول وصلت إلى المرحلة النهائية في الاختراق أو أنني قد وصلت إليها لكن هناك شيء تشعر به في هذه المرحلة بالرغم من كل شيء وهي أن أمور الاختراق أصبحت بمزاجك.

مخترق في القمة: تحول من لقب مخترق إلى لقب مرشد لأمن الإنترنت، وأصبح يقوم بالعمل على كيفية تضلّل المخترقين.

وقد كانت إجابة المخترقين كالتالي: يعتقد ٣٥% من أفراد العينة أنهم مخترقون مستجدون، و ٣٠% يدعون أنهم مخترقون حقيقيون و١٣% يرون أنهم مخترقون في القمة الشكل رقم (٦). وبالنظر إلى مهاراتهم في البرمجة المرتجعة نجد أن نسبة ٥٦% من المخترقين الحقيقتين و٧٣% من المخترقين في القمة لا يعرفون البرمجة المرتجعة وهذا مؤشر على أن نسبة كبيرة منها لم تتمكن من مهارات الاختراق باحتراف إنما يمكن تصنيف أكثرهم على أنهم في بداياتهم ومهاراتهم بسيطة إلى متوسطة.



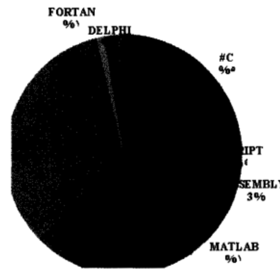
الشكل رقم (٥): المواقع المستهدفة بالهجوم



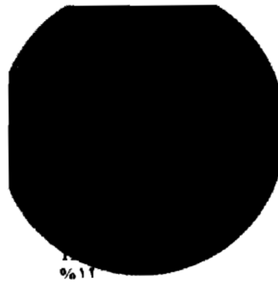
الشكل رقم (٦): تقييم المخترقين لمستواهم

بالنظر إلى الأدوات التي تستخدم في الاختراق؛ فإن النسب متقاربة تتراوح بين ٩% إلى ١٩% أعلى نسبة تساوت فيها أداة أحصنة طروادة وهجوم اليوم الصفري وهي ١٩%، ثم الهجوم الذي يستغل مواطن الضعف بنسبة ١٨%، يليها طريقة الهندسة الاجتماعية وطريقة الاستقصاء بنسبة ١٢%، ثم استخدام برنامج حافظ لنقرات لوحة المفاتيح بنسبة ١١%، وأخيراً جاءت طريقة استخدام الأجهزة المستغلة بنسبة ٩% الشكل رقم (٧). أيضاً أظهرت النتائج أن نسبة إجادة لغة البرمجة هي ٦٥% وقد تنوعت اللغات المعروفة للمخترقين ولكن لغة PHP احتلت النسبة الأعلى حيث بلغت ٢٥% (الشكل رقم ٨). وقد كانت أعلى نسبة لنظام التشغيل المستخدم والمفضل في الاختراق لويندوز بنسبة ٥٢% ويليها في

الترتيب نظام لينكس بنسبة ٣٩%. وكل هذه النتائج تدل على أن أغلبية المخترقين المشاركين في الدراسة هم من المبتدئين أو متوسطي الخبرة.



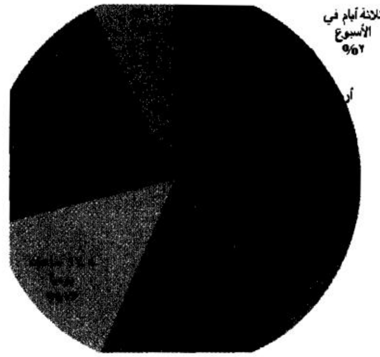
الشكل رقم (٧): أشهر الأدوات المستخدمة في الاختراق



الشكل رقم (٨): أشهر اللغات المعروفة للمخترقين

تبين من الدراسة أن أعلى نسبة للمخترقين من كانت خبرتهم مبنية على التعليم الذاتي وقد بلغت ٨٢% وهذا يدل على قدراتهم المستقبلة في تطوير مهاراتهم والانتقال إلى أطوار أخرى من الاختراق. وقد كانت النسبة الأعلى ٥٩% تستعين بالمواقع والمنتديات التي تهتم بأمور الاختراق كمصدر تعليمي يليها اكتساب الخبرة عن طريق أحد المخترقين بنسبة ٢٣% وبلغت نسبة شراء الكتب المختصة في الأمن ومجال الاختراقات ١٨%.

بالنسبة للمدة التي أمضاها المخترق في الاختراق فقد كانت أعلى نسبة ٤٣% للمدة ٣ سنوات فأكثر تليها المدة من سنة إلى أقل من ٣ سنوات بنسبة ٢٩%. وبينت النتائج أن ٦١% من عينة الدراسة تقضي عدداً من الساعات يومياً في الاختراق أو محاولة الاختراق و٣٢% منهم يمضون عدداً من الساعات أسبوعياً، الجدير بالذكر أن ١٨% من عينة الدراسة يمضون ١٣ ساعة يومياً في محاولة الاختراق. هذا يدل على أن هناك إصراراً وعزيمة واهتماماً من قبل المخترقين بالإضافة إلى أن هناك طاقات تهدر لابد من الاستفادة منها الشكل رقم (٩).



الشكل رقم (٩): المدة التي يقضيها المخترق في محاولة الاختراق

بالنسبة لتفاعل المخترقين مع بعضهم البعض تشير نتائج الدراسة إلى أن ٦٦% من عينة الدراسة تعمل بشكل فردي وأن نسبة ٥٧% لا تشارك بالمنتديات الحوارية وأن نسبة ٣٠% ليس لديها تواصل مع المخترقين و٣٥% لديها تواصل مع عدد لا يتجاوز العشرة. وهذا يدل على أن المخترقين أفراد وليسوا جماعات منظمة، والأفراد عادة أضعف، لكن هذا لا ينفي في وقت من الأوقات تطورهم إلى جماعات فيكون خطرهم أكبر.

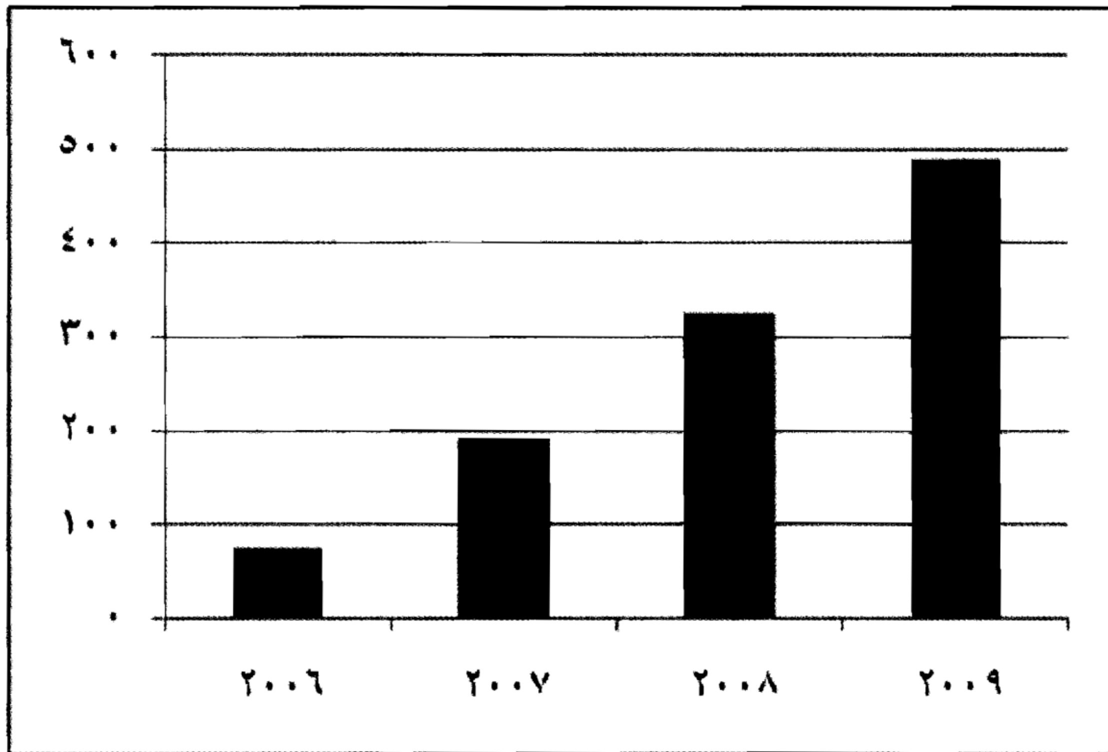
أتضح من نتائج هذه الدراسة أن هناك نسبة تعادل ٤٨% فضلت استغلال موهبة الاختراق في وظيفة في مجال أمن المعلومات وهذا أمر مشجع ولكن ٤٥% من العينة فضلت الاستمرار في الاختراقات وهذا مؤشر مخيف يدعو إلى أخذ الحذر من هذه الفئة. وقد بلغت نسبة الموافقة على إمكانية عقد مقابلة ٤٣% وهي نسبة غير متوقعة مما يعكس رغبة المخترقين في استغلال هذه المهارات في أمور إيجابية.

١- المواقع السعودية المخترقة:

يعتبر موقع زون اتش www.zone-h.org تن من المواقع التي يتم فيها أرشفة المواقع المخترقة وقد جمعت تلك المواقع من شبكة الإنترنت أو أبلغت مباشرة بواسطة المخترقين أنفسهم. ويصنف باعتباره مرجعاً للمواقع المخترقة يسجل فيه أمور من أهمها: وقت الاختراق، كنية المبلغ، رابط الموقع المخترق، وصورة للموقع بعد التشويه تحتوي على رسالة وضعت من قبل المخترق [١٤]. وفيما يلي استعراض لأهم المشاهدات المستخلصة من هذا الموقع:

- بعد رسالة المواقع السعودية التي تم اختراقها في العام الماضي ٢٠٠٩م المسجلة في موقع زون اتش. وجد أن النسبة الأعلى كانت ٤٦% وتستهدف المواقع التجارية (.COM)، يليه المواقع الحكومية (.GOV) بنسبة ٢٠%، ثم المواقع التعليمية (.EDU) بنسبة ٩% الشكل رقم (١١).

- ٢٣٪ من المواقع السعودية المؤرشفة عام ٢٠٠٩م تم مهاجمتها بواسطة مخترق واحد.
- ارتفاع نسبة الهجمات الإلكترونية في عام ٢٠٠٩م ستة أضعاف عما كانت عليه عام ٢٠٠٦م مع توقع زيادة الهجمات في المستقبل. فقد بلغت عدد المواقع السعودية المخترقة في عام ٢٠٠٩م ٤٩١ موقعا، و٣٢٦ موقعاً في عام ٢٠٠٨م، و١٩٢ موقعاً في عام ٢٠٠٧م و٧٥ موقعاً عام ٢٠٠٦م. وتجدر الإشارة إلى أن هذه الإحصائية تركز على المواقع المسجلة تحت النطاق السعودي (sa.) حيث يمكن أن تكون هناك مواقع سعودية مخترقة أخرى لم ترد في هذه الدراسة وذلك كونها مسجلة تحت النطاق العالمي وليس السعودي الشكل رقم (١٠).
- تم اختراق مواقع عالمية كثيرة تهتم بالأمن والحماية وأنظمة الكمبيوتر وعلى رأسها شركة مايكروسوفت وموقع شركة الكاسبرسي من قبل مخترقين سعوديين.
- لم يسلم موقع زون اتش من الاختراق، فقد اخترق عام ٢٠٠٩م ولم تكن هذه هي المرة الأولى التي يتعرض فيها هذا الموقع للهجوم وقد اخترق مرات كثيرة من قبل مخترقين سعوديين.



الشكل رقم (١٠) عدد المواقع السعودية المخترقة والمؤرشفة في zone h



الشكل رقم (١١) المواقع المستهدفة بالهجوم عام ٢٠٠٩م

٢- الخاتمة والتوصيات:

من خلال هذه الدراسة والأفراد المشاركين في الاستبانة يمكننا القول أن معظم المخترقين السعوديين من صغار السن، وقد يكونون في مرحلة الدراسة وهم من الذكور وغير ملتحقين بوظيفة؛ بالإضافة إلى ذلك فإن أغلب أهدافهم الحالية هي الدفاع عن الدين أو الوطن ولا يمتهنون الاختراق بوصفه مصدر رزق، ويعتبر مستواهم في الاختراق مبتدئاً إلى متوسط، ولكن نظراً لارتفاع نسبة الأفراد الذين يجيدون اللغة الإنجليزية وعدد الساعات التي يقضونها في تعلم الاختراق فإن قابليتهم للتطور في الاختراق واردة في المستقبل القريب، مما قد يغير من توجهاتهم وأهدافهم، خاصة وأن قرابة النصف من المشاركين في الدراسة يودون الاستمرار في الاختراق عوضاً عن الالتحاق بوظيفة.

في ضوء ما أسفرت عنه النتائج يمكن التوصل إلى بعض التوصيات القابلة للتنفيذ وهي:

- محاولة الاستفادة من تجارب الولايات المتحدة والصين في اكتشاف الموهوبين من المخترقين وتطوير مهاراتهم وتوظيفهم في مجال أمن المعلومات؛ لسد ثغرات الأنظمة واتخاذ التدابير الوقائية ضد الهجمات الخبيثة؛ عوضاً عن هدر طاقاتهم في الأعمال التخريبية.
- تطوير نظام مراقبة دخول المستخدمين على الإنترنت؛ لأن هناك ثغرات كثيرة يمكن للمخترق استغلالها للوصول إلى الهدف المنشود مثل مقاهي الإنترنت، الشبكات اللاسلكية المفتوحة، وبطاقات الاتصال بالإنترنت وكل تلك الطرق لا تتطلب معرفة هوية المستخدم، مما يتسبب في صعوبة تتبع الاختراقات.

- ضرورة إقامة قسم لأمن المعلومات في القطاعين الحكومي والخاص تحت إدارة مجموعة من المختصين لتفادي هجمات المخترقين.
- الاهتمام بتدريس مقررات أمن المعلومات في كليات علوم الحاسب في الجامعات السعودية ومقررات أخلاقيات الحاسب في التعليم العام والجامعي.

المصادر والمراجع

1- E.Aseev, A.Gostev, "Kaspersky Security Bulletin 2009. Statistics, 2009," Feb. 17,

2010 , Available : http.7/www.viruslist.com/enyanalvsis?pubid-204792098

2- M.Ciampa , Security + Guide to Network Security Fundamentals , 2nd

ed.Canada: Course Technology , 2005.

3- Cheezhead website, Available : http://www.cheezhead.com/20Q9/07/30/ic-

tech-geek-the-government-wants-vou.

4- "Chinese Military Hackers," Available :

http://factsanddetails.com/china.php?itemid=294&catid=8&subcatid=51.

5- "Estonia hit by 'Moscow cyber war*," BBC News, May. 17 , 2007. Available : http://news.bbc.co.**Uk**/2/hi/europe/6665145.stm.

6- A. Greenberg /'Pentagon Seeks High School Hackers,"May.21,2009.Available:

http.//www.forbes. com/2009/05/21/cvbersecuri ty-students-hackers-technology- security-cybersecurity.html.

7- iDefense Security Intelligence Team, "2009 Cyber Threats and Trends," Dec. 12' 2008.

8- **"Netwars Competition," Available : http://www.sans.org/netwars.**

9- "Russian Cyber war on Georgia," Nov. 10' 2008.

Available: http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf.

10- SC Magazine<p.l2 May 2009.

11- Traynor ,"Russia accused of unleashing cyberwar to disable Estonia," The Guardian, May. 17,2007 .Available:

http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

12- "US Cyber Challenge," The Center for Strategic and International Studies (CSIS), Available : http://csis.org/uscc.

13- L.Wilbanks,"When Black Hats Are Really White," IT Pro ,The IEEE Computer Society ,pp. 63-64, Oct 2008.

14- ZONE H , Available : www.zone-h.org.